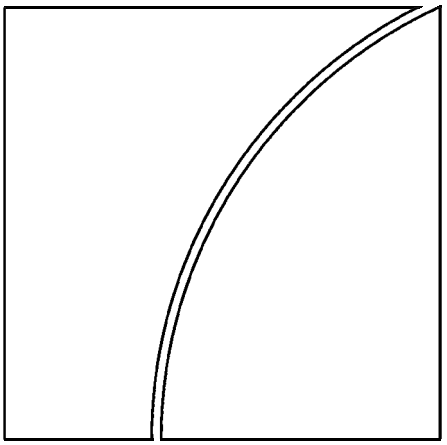
Basel Committee
on Banking Supervision



Implementation of the compliance principles

A survey

August 2008

BANK FOR INTERNATIONAL SETTLEMENTS

Requests for copies of publications, or for additions/changes to the mailing list, should be sent to:

Bank for International Settlements
Press & Communications
CH-4002 Basel, Switzerland

E-mail: publications@bis.org
Fax: +41 61 280 9100 and +41 61 280 8100

ISBN print: 92-9131-773-X
ISBN web: 92-9197-773-X

Contents

Implementation of the compliance principles

A survey

Executive summary

1. In April 2005, the Basel Committee on Banking Supervision[1] released a document entitled *Compliance and the compliance function in banks*[2] (hereafter the Compliance paper). The Compliance paper was intended to provide high-level principles on banks' management of compliance risks, which the Committee defines as "the risk of legal or regulatory sanctions, material financial loss, or loss to reputation a bank may suffer as a result of its failure to comply with laws, regulations, rules, related self-regulatory organization standards, and codes of conduct applicable to its banking activities". As a follow-up to its Compliance paper, the Committee asked its Accounting Task Force to assess the status of implementation of the compliance principles described in this paper, as well as to summarise recent compliance-related incidents and challenges facing the industry regarding compliance issues. This report is based on the results of that assessment, which was conducted in the course of 2007 and in which 21 jurisdictions participated, including the 13 member-jurisdictions of the Basel Committee, and eight other jurisdictions from the Basel Committee's International Liaison Group[3] (ILG).

2. The survey results indicate that in a substantial majority of respondent jurisdictions, banks manage and supervise the compliance function as an important risk management control function, and in line to varying degrees with the Compliance paper. In fact, implementation of the Compliance paper was overwhelmingly considered as having fostered improvements, even where significant non-compliance incidents occurred after its introduction.

3. The survey shows that the high-level principles described in the Compliance paper remain relevant, and are reflected in current supervisory frameworks or in reforms still under way. The publication of the results of this survey is intended to assist jurisdictions that are still working to improve their compliance frameworks by providing them with a range of

---

[1] The Basel Committee on Banking Supervision is a committee of banking supervisory authorities which was established by the central bank Governors of the G10 countries in 1975. It is made up of senior representatives of banking supervisory authorities and central banks from Belgium, Canada, France, Germany, Italy, Japan, Luxembourg, the Netherlands, Spain, Sweden, Switzerland, the United Kingdom and the United States. It usually meets at the Bank for International Settlements in Basel, where its permanent Secretariat is located. More information on the Basel Committee, as well as its publications, can be found at www.bis.org/bcbs/index.htm.

[2] The full version of the 2005 Compliance paper can be found at www.bis.org/publ/bcbs113.htm.

[3] The International Liaison Group provides a forum for deepening the Basel Committee's engagement with supervisors around the world on a broad range of issues. It gathers senior representatives from eight Committee member countries (France, Germany, Italy, Japan, the Netherlands, Spain, the United Kingdom and the United States) and 16 supervisory authorities that are not members of the Committee (Argentina, Australia, Brazil, Chile, China, the Czech Republic, Hong Kong SAR, India, Korea, Mexico, Poland, Russia, Saudi Arabia, Singapore, South Africa and the West African Monetary Union). The European Commission, the International Monetary Fund, the World Bank, the Financial Stability Institute, the Association of Supervisors of Banks of the Americas (ASBA) and the Islamic Financial Services Board are also members of the ILG.

practices, as well as to inform them about the solutions developed to address the main issues faced by jurisdictions who implemented the high-level principles. The results of the survey are for illustrative purposes only and the examples provided herein are not intended to be prescriptive.

4. Of the 21 respondents, 20 reported some form of compliance requirements, even if it is only a component of the overall risk management framework, which demonstrates that the importance of compliance to enhance sound practices in banking organisations is widely recognised. One of the 21 respondents that reported that it did not have any formal compliance requirements does however expect banks to develop a compliance framework and this jurisdiction takes compliance into account in the supervisory process. [4]

5. A large majority of respondents has a compliance framework that follows closely the principles described in the Compliance paper. Of these, eight jurisdictions have a definition of compliance risks that is virtually the same as that used in the Compliance paper while four others either have adopted a principle-based approach with limited detailed requirements, or are following some of the principles now but have not yet developed as comprehensive a framework as described in the Compliance paper. For example, at present, compliance requirements apply only to market activities in one jurisdiction and only in some areas such as money laundering in another.

6. In several jurisdictions, the principles are included in part, but never exclusively, in non-binding guidance as opposed to enforceable requirements. The distinction between binding and non-binding guidance is however blurred.

7. The implementation of the high-level principles is still under way in many jurisdictions: one jurisdiction noted a new framework that had recently been implemented and eight mentioned additional requirements to enter into force by the beginning of 2008.[5]

8. As to the organisation of the compliance function, nearly all respondents impose compliance responsibilities on the board of directors and senior management, thus underlining, as the Compliance paper does, that compliance starts at the top.

9. The four measures most frequently required or recommended by jurisdictions to promote the independence of the compliance function are:

- the appropriate seniority of the head of compliance,
- the specialisation of the compliance function (or at least the prevention of conflicts of interests),
- a formal organisational status, and
- free, unencumbered access to any member of staff or document.

These four measures reflect the four elements described in the paper as forming the basis of the compliance function's independence.

---

[4] This is also the case in another jurisdiction that declined to participate in the survey but gave information on elements of the questionnaire (see paragraph 17).

[5] These include in particular the four last jurisdictions mentioned in the previous paragraph, as well as one of the jurisdictions without a specific compliance framework mentioned above.

10. The core tasks of the compliance function defined in laws, regulations or binding guidance in respondent jurisdictions are "monitoring and testing compliance" as well as "reporting on a regular basis to senior management". The tools most frequently used to promote a strong compliance culture are training and a written policy established by senior management. Many respondents also mentioned the importance of follow-up mechanisms by senior management to ensure that appropriate remedial or disciplinary action is taken if breaches are identified.

11. Certain aspects of the Compliance paper, however, are less frequently included in the respondents' compliance frameworks. For instance, only one-third of respondents mentioned balancing financial performance incentives and compliance incentives as well as mechanisms such as the protection of whistle-blowers among the tools used to promote a strong compliance structure. Similarly, jurisdictions rarely foster the independence of the compliance function by explicitly prohibiting remuneration of compliance function staff based on the financial performance of the business lines for which they exercise compliance responsibilities, although in a limited number of jurisdictions such a prohibition is recommended or implicit. As regards cross-border issues, restrictions still seem to exist to information sharing within groups for compliance purposes: for instance, in some cases, the customer's consent is required.

12. Authorities underlined in their responses two major issues they had to face when implementing a compliance framework. One of these issues, which relates to small and medium-sized institutions in particular, was how banks should organise their compliance function. This includes, for instance, the determination of what are appropriate resources for the compliance function in relation to the size, complexity and nature of the business; the relationship between internal audit and compliance; the independence of the compliance function. Another issue frequently mentioned by authorities was the scope of compliance risks (eg whether the definition covered non-financial rules and regulations).

13. The most frequent areas involved in compliance incidents are market conduct (including conflicts of interests, treating customers fairly and ensuring the suitability of customer advice) as well as prudential laws and regulations. The prevention of money laundering and terrorist financing was also frequently mentioned. Compliance incidents related to accounting and auditing were noted by three jurisdictions. The factors most significantly contributing to these compliance incidents were the failure to introduce, maintain or enforce compliance policies and procedures on a consistent basis throughout the firm; insufficient compliance culture, awareness or training; and a failure to identify or address emerging firm-wide compliance risks.

Introduction

14. As a follow-up to its 2005 Compliance paper, the Committee asked its Accounting Task Force (ATF) to assess the implementation status of the Compliance paper's principles from a banking and supervisory perspective. It also asked the ATF to summarise recent compliance-related incidents and to review the challenges facing the industry regarding compliance issues. In response, the ATF's compliance project team drafted a questionnaire to gather the necessary information from supervisory authorities participating in the survey. The development of the survey also benefited from contributions from other ATF members and members of the International Liaison Group.

15. The questionnaire (see Annex) included questions on:

- the implementation date of a compliance framework;

- the definition of compliance risks;
- existing requirements concerning the organisation of the compliance function;
- the compliance culture;
- cross-border issues and other specific implementation issues; and
- compliance related incidents.

16. Responses from 21 jurisdictions were received in May and June 2007; 13 of which were from Committee member-jurisdictions and eight from other ILG members' jurisdictions.

17. An additional jurisdiction declined to participate, due to the absence of a formal implementation of the Basel paper, even though more broadly formulated compliance requirements exist in the jurisdiction. However, this jurisdiction provided useful information on certain elements of the questionnaire. Where appropriate, these responses are noted below.

The results

1. The existence of a compliance framework

18. Twenty respondents have some form of compliance requirements, even if it is simply a component of the overall risk management framework. However, one respondent as well the jurisdiction which chose not to fully participate in the survey but provided useful information, do not currently have specific compliance requirements, even though they do expect banks to develop a compliance framework and take compliance into account in the supervisory process.

19. Some jurisdictions acknowledged that their existing requirements do not always cover the entirety of the Compliance paper or are specific to certain areas of compliance. For example, at present, compliance requirements apply only to market activities in one jurisdiction and only in some areas such as money laundering in another. Consequently, the implementation of the high-level principles is still under way in many jurisdictions: one jurisdiction mentioned a new framework that had recently been implemented and eight others noted additional requirements to enter into force by the beginning of 2008. Some of these reforms might be prompted by factors other than the Compliance paper, and the European Directive on Markets in Financial Instruments (MiFID) was mentioned several times.

20. Compliance requirements in eight jurisdictions are defined at least in part in laws. However, all eight use additional lower norms: six combine laws with the three other levels of norms (regulations, binding guidance and non-binding guidance), one combines laws and regulations and one combines laws with non-binding guidance.

21. Regulations are the source of compliance requirements in seven jurisdictions. Of these, six use regulations alone and the other combines regulations with non-binding guidance.

22. Binding guidance is used exclusively in five jurisdictions. However, none of the eight jurisdictions that use non-binding guidance relies exclusively on that tool.

2. The definition of compliance risks

23. In twelve jurisdictions (10 Basel Committee members, 2 ILG members), compliance requirements define the expression "compliance risks". The expression is not specifically

defined in two additional jurisdictions but they note that the concept is captured through other aspects of their framework, such as the definition of one or several of the following concepts: legal, regulatory, reputational or market conduct risks.

24. In eight of these twelve jurisdictions, the definition is very close to the one in the Compliance paper:

> *The risk of legal or regulatory sanctions, material financial loss, or loss to reputation a bank may suffer as a result of its failure to comply with laws, regulations, rules, related self-regulatory organization standards, and codes of conduct applicable to its banking activities*.

Another jurisdiction using a concept distinct but similar to compliance risk also uses a definition very close to the one in the Compliance paper. In the four other jurisdictions, the definition is also similar but does not refer however to the *"risk of legal or regulatory sanctions, material financial loss, or loss to reputation"*. Instead, the definition refers directly to not breaching a set of rules and standards.

25. There are, however, slight variations between definitions that may have an impact on the scope of compliance risks. Only five of the eight jurisdictions whose definition is nearly identical to the one in the Compliance paper have kept the idea of "materiality".

26. There are also differences as to the scope of "compliance laws, rules and standards". Whereas all retain laws and regulations, only 10 refer also to other standards such as codes of conducts.

27. The scope of compliance in four jurisdictions includes verifying that the institution's own instructions, policies or internal rules are being followed. The scope of compliance for one jurisdiction includes a reduction in the value of the bank's franchise, or its business potential. This is in addition to sanctions, financial losses and losses that may have resulted due to reputation risks.

28. Supervisors from three jurisdictions limit the scope of compliance risks to laws, rules and standards specific to banking activities. Another jurisdiction refers in its definition of compliance to rules "provided for in banking legislation (ie the banking law and its implementing decrees and regulations), and other legal and regulatory provisions that apply to the banking sector". Yet another jurisdiction has a broadly encompassing definition of compliance risks, but distinguishes between standards that apply to institutions because they provide financial services and standards that apply to all commercial enterprises. For example, labour laws, health codes, building codes and fire safety laws would be requirements with which an institution must comply, but would fall outside of the purview of the institution's compliance function that is subject to review and assessment by the banking supervisor.

29. In other jurisdictions, compliance risks extend to all applicable regulations. In one jurisdiction, however, it is a matter for the institution to decide whether, given the specificities of the activities performed, its compliance function monitors compliance with rules not directly linked to the banking and financial activities in the strict sense, such as rules pertaining to labour law, social legislation, company law or environmental law.

30. The questionnaire asked respondents to identify which of the following six areas are included in their definition of compliance risk:

1. Accounting and auditing requirements;
2. Prudential laws and regulations;

3. Observing proper standards of market conduct, managing conflicts of interest, treating customers fairly and ensuring the suitability of advice to customers;

4. The prevention of money laundering and terrorist financing.

5. Tax laws that are relevant to the structuring of banking products or customer advice;

6. The bank participating knowingly in transactions intended to be used by customers/counterparts to avoid regulatory or financial reporting requirements, evade tax liabilities or facilitate illegal conduct;

31. Among the 14 respondent jurisdictions that define compliance risk, five stated that the approach by areas was not relevant and seven ticked all the six areas proposed. Two other jurisdictions stated that the expression "compliance risks" did not include accounting and auditing requirements. Another also excluded "tax laws that are relevant to the structuring of banking products or customer advice" and "the bank participating knowingly in transactions intended to be used by customers/counterparts to avoid regulatory or financial reporting requirements, evade tax liabilities or facilitate illegal conduct". The three areas always mentioned by respondents as being included in compliance risks are:

- prudential laws and regulations;
- observing proper standards of market conduct, managing conflicts of interest, treating customers fairly and ensuring the suitability of advice to customers;
- the prevention of money laundering and terrorist financing.

32. Five respondents include additional areas in their scope of compliance risks. Some of them explained that it was simply due to their broader definition. Among the examples given are: consumer compliance, fiduciary activities, electronic banking and IT (including outsourcing and web-linking), credit card activities, and competition laws.

33. In one jurisdiction, a bank is responsible for identifying the areas in which compliance risks can arise. The regulation indicates some areas where a bank's exposure to compliance risks can be significantly high. These include prudential laws and regulation as well as observing proper standards of market conduct, including managing conflicts of interest, treating customers fairly and ensuring the suitability of advice to customers.

3. The organisation of the compliance function

34. All 13 Basel Committee member-jurisdictions and seven of the eight non-Committee members of the ILG who participated in the survey prescribe or impose particular requirements regarding the organisation of the compliance function.

a. The responsibilities of the board of directors and senior management

35. In 16 jurisdictions, compliance responsibilities of the board of directors and senior management are defined in law, regulations or enforceable guidance. Four other recommend such responsibilities through non-binding guidance. However, among those four, one explains that the recommendations on the role of the board of directors are compulsory for listed companies under the principle of "comply or explain". Another observes that although no particular structure for a compliance management system is prescribed, institutions are expected to establish and maintain one which is commensurate with their size, complexity and risks, and that significant weaknesses in the compliance function could be the basis of an enforcement action.

b. The independence of the compliance function

36. The questionnaire listed six measures recommended by the Compliance paper as ways to promote the independence of the compliance function. These are:

1. Requiring a head of compliance to be appointed (i.e. an executive or senior staff member with overall responsibility for co-ordinating the identification and management of the bank's compliance risk and supervising other compliance function staff);
2. That compliance function staff perform only compliance responsibilities (or, where this is not practicable because of the small size of the entity, that appropriate measures be taken to avoid potential conflicts of interest);
3. Requiring that the compliance function be given the right, on its own initiative, to communicate with any staff member and obtain any records or files necessary to enable it to carry out its responsibilities;
4. Requiring the compliance function to be given a formal status within the bank (responsibilities, independence, access to information, direct access to the board of directors or a committee of the board, ...);
5. Prohibit remuneration of compliance function staff that is related to the financial performance of the business lines for which they exercise compliance responsibilities; and
6. That the supervisor and the board of directors be informed of the departure of the head of compliance and the reasons for such departure.

37. Among these six, measures 1 through 4 are more frequently implemented, each being required by 14 or 15 jurisdictions and recommended by two to four other respondents.

38. However, regulations and guidance rarely go into more details and the two other measures were less frequently mentioned by respondents: only seven jurisdictions prohibit remuneration of compliance function staff that is related to the financial performance of the business lines for which they exercise compliance responsibilities (no. 5 above), even if three additional jurisdictions recommend such a prohibition in non-binding guidance. In one jurisdiction the prohibition is not a hard-and-fast rule.[6] Conversely, three further jurisdictions do not explicitly have or recommend a prohibition, but consider that the general independence requirement may restrict to some extent the possibility to have such a link between remuneration and the performance of the business lines. Another notes that such a matter (as well as access to information) is not explicitly required but is raised at the annual meetings the supervisor has with heads of compliance.

39. Similarly, only nine jurisdictions require and one recommends that the supervisor and the board of directors be informed of the departure of the head of compliance and the reasons for such departure (no. 6 above).

[6] This supervisor promotes in its guidelines two levels of compliance function: (1) Operational, ie in business, where the supervisor would not object to remuneration tied to financial performance, and (2) Oversight, that is independent of business. The supervisor would object to bonus remuneration tied primarily to financial performance.

40. Looking at the combination of measures used to promote the independence of the compliance function:

- 11 jurisdictions impose[7] five or six of the six measures noted above in paragraphs 35 to 37;
- Four jurisdictions impose three or four of these measures (one of these recommends the other measures);
- Three jurisdictions recommend[8] four or five measures;
- One does not prescribe nor recommend any of them, simply requiring that "the compliance function should be independent";
- Two did not respond to this part of the questionnaire; however, one of them indicated that although there was no comprehensive compliance function, some aspects were covered by specific regulations.

c. The resources of the compliance function

41. In 14 jurisdictions compliance requirements include the resources of the compliance function, while five other jurisdictions address resources in their non-binding guidance.

42. Several jurisdictions insisted in their comments, as the Compliance paper does, on the qualitative aspects of resources (skills, experience, etc). Five jurisdictions mentioned proportionality, in most cases referring to the size of operations as well as their nature and complexity.

43. One respondent's regulations prohibit outsourcing the compliance function to third parties, without however precluding the possibility to use the expertise or technical means of third parties. Another jurisdiction explained that the compliance function should have the authority and financial resources to appoint outside consultants on specific and complex innovations in the applicable laws or regulations and/or in the bank's operations.

d. Tasks performed by compliance

44. Fifteen jurisdictions define the responsibilities of the compliance function in their laws, regulations or binding guidance while two do so only in non-binding guidance.

45. The questionnaire described seven different responsibilities of the compliance function (that, however, do not need to be all carried out by a "compliance department" or "compliance unit", but can be exercised by staff in different departments). These seven areas were all taken from the Compliance paper and include:

- advising senior management on compliance laws, rules and standards
- providing guidance and educating staff
- identifying, measuring and assessing compliance risk
- the development of new products and new business practices

---

[7] One jurisdiction specified that the "requirements" are stated more broadly, as expectations.

[8] One jurisdiction observes that some elements are included in the anti-money laundering / countering the financing of terrorism (AML/CFT) framework and are enforceable.

- monitoring and testing compliance
- reporting on a regular basis to senior management on compliance matters
- the establishment of a compliance programme

46. Ten jurisdictions mentioned all seven responsibilities while four jurisdictions use requirements to establish these responsibilities, and six use recommendations or a mix of requirements or recommendations.

47. Seven jurisdictions mentioned five or six of the seven responsibilities.

48. One respondent defines only two tasks in regulations, due to its principle-based approach.[9]

49. Responses show that the tasks most frequently defined in laws, regulations or binding guidance are "monitoring and testing compliance" as well as "reporting on a regular basis to senior management". Three other tasks, namely "advising senior management on compliance laws, rules and standards", "providing guidance and educating staff", and "identifying, measuring and assessing compliance risk" are also frequently defined through enforceable means. When adding cases where non-binding guidance is used, each of these five tasks is mentioned by 16 to 18 respondents.

50. The development of new products and new business practices and the establishment of a compliance programme are less frequently mentioned (13 jurisdictions each). One jurisdiction explained that the supervisory authority raises these two matters at the annual meeting with the compliance function or senior executive responsible for compliance in the bank, but it is not explicitly documented in laws or regulations.

e. Relationship with internal audit

51. The relationship between the compliance function and internal audit is addressed by 12 jurisdictions in their laws, regulations or binding guidance while five do so in their non-binding guidance. One did not respond. Three jurisdictions do not address the issue, but one of them specified that regulations distinguish internal audit and compliance.

4. Promoting a strong compliance culture

52. The tools most frequently used to promote a strong compliance culture are training and the existence of a written policy established by senior management. Follow-up mechanisms by senior management to ensure that appropriate remedial or disciplinary action is taken if breaches are identified were also mentioned by 13 jurisdictions.

53. Only one-third of respondents mentioned the balance between financial performance incentives and compliance incentives, as well as mechanisms such as the protection of whistle-blowers. The proportion is slightly higher for Committee members.

[9] The three remaining jurisdictions did not provide a response: one specified that it was due to the fact that existing requirements do not cover all areas; one does not yet have any specific compliance requirements; and the other indicated that it followed a principle-based approach.

5. Cross border issues

a. Access of group head offices to data in branches and subsidiaries

54. The questionnaire explored whether there were restrictions on branches and subsidiaries of foreign banks sharing information with head office compliance oversight groups. Five jurisdictions answered that there were no restrictions and one of these explained that in its banking legislation, branches and subsidiaries of foreign banks are regarded as "extensions" of head office. This means that head office has right of access to all information related to the branches and subsidiaries established in the jurisdiction. Transmissions to third parties are, however, restricted (excepted in the cases mentioned hereunder). In another jurisdiction, although there are no restrictions as a general principle, there should be a good business reason for sharing information with the head office.

55. The response in eight jurisdictions was that the extent to which locally gathered customer personal data may be sent to the jurisdiction of the head office depends on the level of data protection in that jurisdiction (the home jurisdiction). Three respondents specified that the level of data protection in the home jurisdiction simply had to be appropriate; one noted that it should be similar; and three stated that it had to be equivalent. For one of the latter jurisdictions, however, when the level of data protection is not equivalent, it is necessary to get a specific authorisation for international data transfer. This authorisation is not necessary in case of international judiciary, or other public authority request.

56. Restrictions on the ability of the head office to redistribute host jurisdiction customer personal data to third parties were specified in nine jurisdictions but they added that there were exceptions allowing information to be transmitted to banking supervisors (except in three cases), to the judiciary, upon an appropriate court order (except in three jurisdictions) and to Financial Intelligence Units – FIUs (except in four jurisdictions). Of the jurisdictions not allowing exceptions, one specified that data transmission remains possible with the customer's consent and further specified that "banking supervisors can obtain information directly from the branch without going through the head office" and that "branches [in the jurisdiction] are required to make suspicious transaction reports directly to the [local] FIU."

57. As regards suspicious transaction reports (STRs), another jurisdiction requires organisations not to disclose STRs to affiliates (whether domestic or foreign), and permits disclosure to foreign parent companies or head offices only where appropriate confidentiality arrangements are put in place to restrict further disclosure. There is no restriction on sharing (with domestic or foreign affiliates, parent companies or head offices) information about customers and transactions reported on STRs, provided that institutions do not disclose a STR itself or information that would disclose that a STR has been filed.

58. A response from one jurisdiction mentioned other restrictions that did not, however, prevent the head office from using the information for compliance oversight and risk management. Another jurisdiction explained that personal data can only be exchanged through regulatory channels and with the existence of a memorandum of understanding (MOU).

59. Responses from two jurisdictions indicated that the customer had to be informed of the possibility that his data may be transmitted to the head office for compliance purposes, and four indicated that the customer's approval was necessary. Of these, two indicated that this approval was not necessary in all circumstances (one of them mentioning in particular data sharing in European Union jurisdictions as well as further possibilities to transmit data with the permission of the domestic authority in charge of data protection). Of these two, one further explained that the whole issue was extremely complex, that the answers gave only

first indications and had to be considered with extreme care. Another specified that the customer's consent was in principle required for both branches and subsidiaries.

60. An additional jurisdiction requires financial institutions to give consumers an option to restrict the sharing of certain consumer-specific information with affiliated institutions. Consumers may not restrict, however, the sharing of information between affiliated financial institutions related to transactions and the institution's experience with the particular consumer. In another jurisdiction, under privacy laws and subject to limited exceptions that are tied to the public interest, use and disclosure of personal information is subject to the informed consent of the person.

61. One jurisdiction did not respond to this part of the questionnaire, simply stating that "the treatment of any data shared with head office will need to be compliant with data protection requirements."

b. Access of home jurisdiction supervisors to information in foreign branches and subsidiaries

62. In 16 jurisdictions, there are no restrictions on the access of home jurisdiction supervisors to examine the operations of locally established branches of subsidiaries with regard to compliance with head office compliance policies. Of these respondents, nine reported that this was provided an MOU exists with the foreign supervisor, and/or on a reciprocal basis, and/or with prior approval of the host jurisdiction regulator.

63. An additional jurisdiction stated that examinations of cross-border establishments by their home jurisdiction supervisors are subject to the protocols set forth in Basel Committee documents and bilateral arrangements, as well as host supervisor policies and procedures. As a general rule, examinations are undertaken only after prior notification and consultation with the licensing or host supervisory authority and the host supervisor reserves the right to participate in such examinations and/or limit disclosure of customer information to home jurisdiction supervisors. Another jurisdiction also allows access to home jurisdiction supervisors provided that they are subject to professional secrecy provisions, the information is used only for prudential purposes, and that information can be transmitted to a third party only with the agreement of the host supervisor. This jurisdiction also specified that information relating directly or indirectly to asset management can be collected, and the host supervisor will conduct the inspection for the home jurisdiction supervisor and transmit the indications in compliance with the law on "administrative procedure". In two other jurisdictions other restrictions exist (prior consent of the customer in one case and, in the other, requirement to demonstrate a legitimate interest and on the condition that it is not foreseeable that the knowledge of the information may cause a monetary damage to the customer). One jurisdiction did not answer.

6. Issues encountered in implementing compliance requirements

64. Authorities underlined in their responses two major issues they had to face when implementing a compliance framework. One of these issues, of particular significance for small and medium-sized institutions, was how banks should organise their compliance function. This includes, for instance, the determination of what are appropriate resources for the compliance function in relation to the size, complexity and nature of the business; the relationship between internal audit and compliance; and the independence of the compliance function. Another issue frequently mentioned by authorities was the scope of compliance risks (eg whether the definition covered non financial rules and regulations). Those two issues were mentioned by 11 and 9 respondents, respectively. The proportionality of the compliance framework was also mentioned by seven respondents. One jurisdiction

commented in that regard on the challenge to craft compliance requirements that can be understood and implemented in a cost-effective manner by all institutions, from the very small ones to the very large and complex ones. The level of detail of the requirements (eg principle-based or more detailed) was raised only by four respondents, and the involvement of the board of directors by three respondents.

65. Other difficulties mentioned include the shift in culture. As regards the level of detail, several respondents noted that some banks (especially the smaller ones, in one jurisdiction,) had asked for more guidance (eg how many independent compliance oversight staff are necessary for that bank in those circumstances), whereas other banks complained that the guidance is too prescriptive, despite being general, principles-based and focused on risk management. For one respondent, the only issue was whether banks needed to set up duplicate reporting lines to the board for operational and compliance risk reporting. In another, the issue of "whistle blowing" was very difficult, and was in the end not included in regulations, even if a legislative amendment is envisaged for all major companies, not only banks.

66. Two jurisdictions considered that there had been no major issues, and two others distinguished the case of large international banks, where implementation had not been an issue, and the case of smaller institutions.

67. To facilitate effective implementation, solutions included issuing guidance to explain the requirements; monitoring closely implementation and encouraging banks to make progress; and conducting intensive discussions with banks (one jurisdiction used this instead of best practice that banks tend to consider as prescriptive), either on an individual basis or with industry associations. An important objective of individual contact is to find proportionate solutions for each bank. Another means to achieve this objective was to insist on the ability of the firm to demonstrate the effectiveness of its framework, taking into account the size and complexity of the institution. Giving time to adapt gradually was also mentioned several times. For instance, one jurisdiction gave banks 12 months from the issuance of regulation to ensure a full separation of the compliance function and the internal audit function.

7. Compliance incidents

68. Respondents were asked whether major compliance-related incidents at banks had taken place within their jurisdiction within the past two years. Responses from nine jurisdictions provided cases and a few others simply gave some general characteristics concerning the main compliance incidents.

69. The most frequent areas of compliance involved are market conduct (including conflicts of interests, treating customers fairly and ensuring the suitability of advice to customers) as well as prudential laws and regulations (eight respondents each). The prevention of money laundering and terrorist financing was also frequently mentioned (six respondents). Accounting and auditing was involved in three jurisdictions.

70. The most significant contributing factors were the failure to introduce, maintain or enforce compliance policies and procedures on a consistent basis throughout the firm, an insufficient compliance culture, awareness or training, as well as a failure to identify or address emerging firm-wide compliance risks.

71. In five cases, respondents indicated that in general, compliance incidents had taken place after the implementation of specific compliance requirements. However, in three jurisdictions, the incidents had occurred before the issuance of such requirements, and in two jurisdictions, after requirements had been introduced, but before their implementation.

72. Responses from 12 jurisdictions indicated that the introduction of compliance requirements and the corresponding implementation of those requirements in banks had influenced the number, nature or seriousness of reported compliance incidents. Three other respondents considered that it was not the case while six did not answer.

Most significant contributing factors	Number of compliance-related incidents
● Insufficient Board oversight	4
● Insufficient involvement by Senior Management in compliance matters	6
● Failure to introduce, maintain or enforce compliance policies and procedures on a consistent basis throughout the firm	10
● Failure to identify or address emerging firm-wide compliance risks	7
● Lack of independence of the compliance function	2
● Inadequate resources of the compliance function	5
● Imbalance between financial performance incentives and compliance incentives	3
● Insufficient compliance culture, awareness or training	8
● Cross border issues	4
● Other causes	1

73. In 11 cases, respondents identified a significant trend where organisations in their jurisdiction have made enhancements to compliance risk management and oversight in response to the Compliance paper. One specified that the paper had had an influence through industry organisations, another that the influence was due to the paper being implemented in domestic regulations. Another explained that the paper had helped in promoting compliance culture across the firms, as well as in mapping compliance risks (ie identifying precisely, measuring and monitoring risks of non-compliance). In one case, a respondent noted a significant upward trend in the allocation of resources to compliance functions; the seniority of compliance management staff; and the integration of compliance and broader risk management control functions. Progress in the areas of integrity and AML were also observed.

74. The response from four jurisdictions noted that there was no such observable trend, some of them explaining that the principles contained in the paper had already been included in their regulations, or that the causes of such an evolution were difficult to identify. No responses were received from five jurisdictions.

The ATF Compliance Project Team

Team Leader:
Mr Hiroshi Ohata
Financial Services Agency, Japan

Commission bancaire, financière et des assurances, Belgium	Mr Marc Pickeur
Banco Central do Brasil	Mr Amaro Luiz de Oliveira Gomes
Office of the Superintendent of Financial Institutions, Canada	Ms Joan Bentley
Commission Bancaire, France	Mr Laurent LeMouël
Deutsche Bundesbank, Germany	Mr Raoul Nägele
Bundesanstalt für Finanzdienstleistungsaufsicht, Germany	Mr Markus Grund
Banca d'Italia	Ms Maria Antonietta Antonicelli
Bank of Japan	Mr Tetsushi Miyaji
Commission de Surveillance du Secteur Financier, Luxembourg	Mr Edouard Reimen
De Nederlandsche Bank, Netherlands	Mr Maarten Hage
Banco de España, Spain	Mr Pedro Comin Rodriguez
Finansinspektionen, Sweden	Mr Johan Grönquist
Financial Services Authority, United Kingdom	Mr Andrew John Sheen
Board of Governors of the Federal Reserve System, United States	Ms Nina Nichols
Federal Reserve Bank of New York, United States	Mr Jonathan Polk
Office of the Comptroller of the Currency, United States	Mr Calvin R. Hagins
Federal Deposit Insurance Corporation, United States	Mr Robert Storch
Senior Advisor on Accounting and Auditing Policy, ATF	Mr Jerry Edwards
Bank for International Settlements	Mr Rory Macfie
Secretariat, Basel Committee on Banking Supervision	Mr Stéphane Mahieu

Annex

Survey questionnaire

The questions used for this report are presented here.

ATF Compliance project team

Questionnaire on the implementation of compliance requirements for banks and the Basel Committee paper "Compliance and the compliance function in banks"

1. Your authority

(a) Country name:

please select from the list

(b) Please specify the name of your authority:

(c) Please specify he name and email address of a contact person at your authority for questions concerning the responses to this survey:

2. The compliance framework in your jurisdiction

(a) Are there existing or proposed specific requirements for the management of compliance risk by banks in your jurisdiction?

- Yes
- No

(b) If so, when were they introduced, or when are they proposed to be introduced?

(please insert a date with the following format: dd/mm/yyyy)

(c) Are the compliance requirements consistent with the principles contained in the Basel Committee's compliance paper?

- Yes
- No

(d) If they are not consistent, in what areas do they diverge?

(e) Are there any plans to address specific divergences?

- Yes
- No

(f) If not, please state here the reasons why:

(g) Where are compliance requirements defined?

- ☐ in laws
- ☐ in regulations
- ☐ in enforceable guidance or codes of conduct
- ☐ in non binding guidance or codes of conduct

Please note: for the purposes of this questionnaire, guidance or codes of conduct are considered to be "enforceable" where non-compliance could result in enforcement action taken by a supervisory authority or self regulatory organisation.

(h) Please specify here the source(s) of such requirements (reference to the relevant laws, decrees, regulations, etc). If possible, please provide a link to the relevant texts or join them in a separate file (preferably, if available, an English version or translation).

(i) You may provide here any additional information related to questions 2 (a) to (h):

3. The definition of compliance risk in your jurisdiction

(a) Do the compliance requirements in your jurisdiction define the expression "compliance risk"?

- ☐ Yes
- ☐ No

(b) If so, please provide here the definition :

(c) Please specify whether this definition limits the scope of compliance risk:

- ☐ by reference to identified laws, rules and standards
- ☐ to laws, rules and standards specific to banking activities

- [ ] to laws, rules and standards that are material as regards the bank's risk of legal or regulatory sanctions, material financial loss or loss of reputation
- [ ] other
- [ ] not applicable

If other, please specify:

(d) If the expression "compliance risk" is defined in your jurisdiction, which of the following areas does it cover?

- [ ] approach by area is not relevant
- [ ] accounting and auditing requirements
- [ ] prudential laws and regulations
- [ ] observing proper standards of market conduct, managing conflicts of interest, treating customers fairly and ensuring the suitability of customer advice
- [ ] the prevention of money laundering and terrorist financing
- [ ] tax laws that are relevant to the structuring of banking products or customer advice
- [ ] the bank participating knowingly in transactions intended to be used by customers/counterparts to avoid regulatory or financial reporting requirements, evade tax liabilities or facilitate illegal conduct
- [ ] any other areas

If other please specify here:

Please provide here any explanation related to this section

4. The organisation of the compliance function

(a) Does your jurisdiction prescribe or impose particular requirements regarding the organisation of the compliance function?

- [ ] Yes
- [ ] No

(b) If yes, please specify whether such requirements cover:

(i) the responsibilities of the board of directors and senior management?

please select from the list

If so, how?

(ii) the independence of the compliance function?

☐ Yes

☐ No

In particular are there provisions:

● requiring a head of compliance to be appointed (i.e. an executive or senior staff member with overall responsibility for co-ordinating the identification and management of the bank's compliance risk and supervising other compliance function staff)

please select from the list

● requiring the supervisor and the board of directors to be informed of the departure of the head of compliance and the reasons for such departure

please select from the list

● requiring compliance function staff to perform only compliance responsibilities (or, where this is not practicable because of the small size of the entity, that appropriate measures be taken to avoid potential conflicts of interest)

please select from the list

● prohibiting remuneration of compliance function staff that is related to the financial performance of the business lines for which they exercise compliance responsibilities

please select from the list

● requiring that the compliance function be given the right, on its own initiative, to communicate with any staff member and obtain any records or files necessary to enable it to carry out its responsibilities

please select from the list

● requiring the compliance function to be given a formal status within the bank (responsibilities, independence, access to information, direct access to the board of directors or a committee of the board, ...)

please select from the list

Please provide here any additional information regarding the independence of the compliance function:

(iii) the resources of the compliance function?

please select from the list

Please provide here any additional information:

(iv) the responsibilities of the compliance function?

please select from the list

In particular are there provisions in your jurisdiction prescribing the responsibilities of the compliance function concerning:

● advising senior management on compliance laws, rules and standards

please select from the list

● providing guidance and educating staff

please select from the list

● identifying, measuring and assessing compliance risk

please select from the list

● the development of new products and new business practices

please select from the list

● monitoring and testing compliance

please select from the list

- reporting on a regular basis to senior management on compliance matters

please select from the list

- the establishment of a compliance programme

please select from the list

Please provide here any additional information:

(v) the relationship with the internal audit function?

please select from the list

Please provide here any additional information:

5. Promoting a strong compliance culture

(a) Does your jurisdiction prescribe or impose particular requirements (beyond those described in Section 4 above) with respect to promoting a strong compliance culture within banks in your jurisdiction?

- ☐ Yes
- ☐ No

If yes, please describe these requirements

(b) In particular do these requirements include:

- ☐ the obligation for senior management to establish a written compliance policy
- ☐ compliance training requirements adapted to the responsibilities of staff members
- ☐ follow-up mechanisms by senior management to ensure that appropriate remedial or disciplinary action is taken if breaches are identified
- ☐ ensuring an appropriate balance between financial performance incentives and compliance incentives (eg: compensation tied to compliance)
- ☐ prescribing a mechanism through which any member of the bank's staff can report compliance issues in confidence, without fear of prejudice or retaliation (eg: protection of whistle-blowers)

6. Cross-border issues

(a) What, if any, are the restrictions on branches and subsidiaries of foreign banks established in your jurisdiction sharing information with head office compliance oversight groups?

☐ (i) no restrictions

☐ (ii) the extent to which locally gathered customer personal data may be sent to the jurisdiction of the head office depends on the level of data protection in that jurisdiction (the home jurisdiction). If so, is the level of data protection in the home jurisdiction required to be:

- ☐ equivalent to the host country level of data protection
- ☐ similar to the host country level of data protection
- ☐ appropriate

☐ (iii) restrictions on the ability of the head office to redistribute host country customer personal data to third parties. If so, are there exceptions allowing information to be transmitted to:

- ☐ banking supervisors
- ☐ the judiciary, upon an appropriate court order
- ☐ financial intelligence units*

**financial intelligence units are the national centre for the receiving, analysing and disseminatinig of suspicious transactions reports regarding potential money laundering or terrorist financing (FATF recommendation 26)*

☐ (iv) other restrictions on the use by head office of host country customer personal data. If so is the head office nevertheless authorised to use the information for compliance oversight and risk management?

- ☐ Yes
- ☐ No

☐ (v) the host country customer has to be informed of the transmission of his/her personal data to head office. If so, please specify whether this requires that :

- ☐ the customer be informed of the possibility of such transmission
- ☐ the customer be specifically informed before each transmission
- ☐ the approval of the customer be obtained

☐ (vi) other restrictions

If other, please specify:

(b) Please provide here any other explanation related to question (a):

(c) Are there any restrictions in your jurisdiction on the access of home country supervisors to examine the operations of locally established branches of subsidiaries with regard to compliance with head office compliance policies?

- ☐ Yes
- ☐ No

Please explain:

7. Specific issues encountered in implementing compliance requirements for banks

(a) Please describe here any specific issues encountered when introducing compliance requirements for banks in your jurisdiction.

(b) In particular did those issues concern:

- ☐ the scope of compliance risk
- ☐ the level of detail of the requirements (eg: principle based or more detailed)
- ☐ the organisation of the compliance function
- ☐ the proportionnality of the compliance framework
- ☐ the involvement of the Board (or of an appropriate board level committee)

(c) Which solutions have been adopted to address those issues?

8. Compliance related incidents

(a) If there have been any major compliance-related incidents at banks within your jurisdiction within the past two years, please identify in the chart below (column A):
● the most significant contributing factors to such incidents
● any specific areas of compliance that were involved in such incidents
● whether the incidents occured before or after the implementation of suitability requirements
You may also use the same chart (columns B, C and D) as well as the comment boxes in question 8 (b) to describe a few examples of recent individual compliance-related incidents (there is no need to mention names).

	(A) General situation	(B) Case 1	(C) Case 2	(D) Case 3
Most significant contributing factors				
● Insufficient Board oversight	☐	☐	☐	☐
● Insufficient involvment by Senior Management in compliance matters	☐	☐	☐	☐
● Failure to introduce, maintain or enforce compliance policies and procedures on a consistent basis throughout the firm	☐	☐	☐	☐
● Failure to identify or address emerging firm-wide compliance risks	☐	☐	☐	☐
● Lack of independence of the compliance function	☐	☐	☐	☐
● Inadequate resources of the compliance function	☐	☐	☐	☐
● Imbalance between financial performance incentives and compliance incentives	☐	☐	☐	☐
● Insufficient compliance culture, awareness or training	☐	☐	☐	☐
● Cross border issues	☐	☐	☐	☐
● Other causes	☐	☐	☐	☐
If other, please specify:				
Areas of compliance involved				
● accounting and auditing	☐	☐	☐	☐
● prudential laws and regulations	☐	☐	☐	☐
● market conduct, conflict of interest, treating customers fairly and ensuring the suitability of customer advice	☐	☐	☐	☐
● the prevention of money laundering and terrorist financing	☐	☐	☐	☐
● tax laws that are relevant to the structuring of banking products or customer advice	☐	☐	☐	☐
● other areas	☐	☐	☐	☐
If other, please specify:				
Please indicate whether they occured:				
● before specific compliance requirements were issued	☐	☐	☐	☐
● after specific compliance requirements were issued, but before the requirements were implemented within the firm concerned	☐	☐	☐	☐
● after the implementation of specific compliance requirements within the firm concerned	☐	☐	☐	☐

(b) You may describe further hereunder the examples of compliance related incidents:

►Case 1

►**Case 2**

►**Case 3**

(c) In your view, has the introduction of compliance requirements in your jurisdiction and the corresponding implementation of those requirements in banks under your supervision had any effect on the number, nature or seriousness of reported compliance incidents?

- ☐ Yes
- ☐ No

(d) If your answer to the previous question is "yes", please describe further the effect of the introduction of such requirements

(e) Can you identify any significant trends where organisations in your jurisdiction have made enhancements to compliance risk management and oversight in response to the compliance paper?

- ☐ Yes
- ☐ No

Please explain:

(f) You may provide here any additional information related to section 8